RNK COMMUNICATIONS

February 28, 2008

VIA ECFS

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, DC 20554

Re: Annual Customer Proprietary Network Information Compliance Certification; EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. §64.2009(e), RNK, Inc. ("RNK") hereby submits its Annual Customer Proprietary Network Information ("CPNI") Compliance Certification. Should you have any questions regarding this submission, please direct them to the undersigned at (781) 613-9148, or e-mail mtennis@rnkcom.com.

Sincerely,

Matthew Tennis
Counsel

Cc: Enforcement Bureau, Telecommunications Consumers Division via UPS overnight delivery (2)
Best Copy and Printing, Inc. via email (1)

RNK COMMUNICATIONS

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 28, 2008

Name of company covered by this certification: RNK, Inc.

Form 499 Filer ID: 820199

Name of signatory: Richard N. Koch

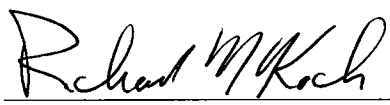
Title of signatory: President

I, Richard N. Koch, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules (see attachment A).

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed  [/Richard N. Koch/]

Richard N. Koch/President

Attachment A

Statement of RNK Compliance Procedures

1. **RNK Use of CPNI:** RNK's operating procedures ensure that RNK is in compliance with the Commission's CPNI Rules. Except as required or permitted by law or Subpart U of Title 47 of the Code of Federal Regulations; 47 CFR 64.2001, et seq., RNK does not use CPNI.

   RNK has internal policies and procedures in place to educate employees as to the confidential nature of CPNI and when disclosure of CPNI is appropriate. RNK's Employee Manual, which employees are required to review and abide by, includes express policies detailing RNK's use of CPNI and identifying its proprietary nature. RNK customer service personnel have also been instructed in the proper usage and protection of CPNI when dealing with customer service requests. Further, RNK's Master Service Agreement, available to the public on its company website, includes express provisions referencing RNK and its business partners' use of CPNI and identifying both the proprietary nature of CPNI and the necessity to safeguard such information. In addition, RNK does not use or otherwise disclose CPNI for marketing purposes. Finally, RNK releases CPNI pursuant to lawfully executed instruments or authorizations, and in limited circumstances as described in Section 2.

2. **Carrier Authentication Requirements:** Presently, RNK does not disclose CPNI over the phone when customers call RNK. If a customer requests CPNI, and does not have an online account, procedures are in place to allow RNK employees to coordinate internally with legal and regulatory departments to carry out disclosure on a case-by-case basis in accordance with the CPNI Rules. RNK may provide CPNI to a requesting customer in such instances through contacting that customer using their address of record information. These procedures ensure that customers can receive information related to their services with minimal risk of unauthorized disclosure of CPNI. Customers with online accounts can also access CPNI through the use of a username/password combination.

   Certain RNK business customers access CPNI using an online, automated system. Only unique customer servers are recognized by RNK's system, based in part on the server's physical location. While RNK believes this method of disclosure is equivalent to, if not more secure than, password protection, and even though RNK, as a small business entity, is not obligated to comply with online carrier authentication requirements until June 8, 2008, RNK has put into place notice and contractual procedures to ensure that each business customer who acquires CPNI by this method is aware of the CPNI Rules and also agrees to safeguard CPNI in accordance therewith. RNK believes that it will be fully compliant with the online carrier authentication requirements by the June 8, 2008 deadline.

3. **Notice of Account Changes:** RNK customers are notified whenever changes occur in their accounts, such as password or address of record changes, generally via email notification.

4. **Notice of Unauthorized Disclosure:** RNK's operating procedures ensure that RNK is in compliance with the Commission's CPNI Rules regarding unauthorized disclosure of CPNI. In the event an RNK employee suspects an unauthorized disclosure of CPNI has occurred, RNK's internal procedures provide that the employee notify their supervisor, who coordinates with RNK's legal and regulatory departments to determine if a breach has occurred. In the event of breach, RNK's procedures provide that its legal and regulatory departments notify the United States Secret Service (USSS) and the FBI within seven business days through the online central reporting facility, and proceed according to the CPNI Rules.

   RNK has put into place procedures to maintain records of unauthorized disclosures of CPNI, notifications to the USSS and the FBI regarding those disclosures, as well as the USSS and the FBI response to the notifications for a period of at least two years. These records will include the following, if available, for each unauthorized disclosure: the date RNK discovered the unauthorized disclosure, the date notice was sent to the USSS and FBI, a detailed description of the CPNI that was disclosed, and any other circumstances of the disclosure not covered under the above.

5. **Opt-in/Opt-out Procedures:** Presently, RNK does not utilize CPNI, for sales or marketing purposes, that would require the use of opt-in or opt-out procedures as described in the CPNI Rules.

6. **RNK Internal Policy and Disciplinary Policy:** RNK has adopted a policy requiring employees to comply with the CPNI Rules. RNK's policy provides that any employee who fails to comply with the Rules and RNK's internal policies is subject to severe disciplinary procedure, up to and including immediate termination depending on the nature of the offense and whether or not the noncompliance was intentional.